THE HONORABLE RICHARD A. JONES

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. ROMAN SELEZNEV, Defendant.	No. CR 11-70RAJ MOTION TO SUPPRESS **EVIDENTIARY HEARING: June 1, 2016**

I. INTRODUCTION

The Defendant, Roman Seleznev, by and through his attorneys, John Henry Browne and Emma C. Scanlan, respectfully requests that the Court suppress all evidence obtained from the Sony Vaio laptop that was seized on July 5, 2014. This request is based on the following three grounds: (1) the affidavit submitted in support of the application to search the laptop relied on stale information that fails to establish probable cause to search the laptop; (2) the 23-day delay in applying for a warrant to search the laptop was, under the circumstances of this case, an unwarranted delay that prejudiced the rights of Mr. Seleznev by creating an opportunity for the data on the laptop to be altered; and (3) the laptop was so mishandled by the United States Secret Service ("USSS") during the 23-day period between when it was seized and when it was imaged – whether intentionally or as a consequence of gross incompetence – that all evidence obtained from the laptop should be excluded.

LAW OFFICES OF JOHN HENRY BROWNE, P.S.
200 DELMAR BUILDING
108 SOUTH WASHINGTON STREET
SEATTLE, WASHINGTON 98104
(206) 388-0777 • FAX: (206) 388-0780

II. RELEVANT FACTS

A. Seizure and Search Warrant Affidavit

On July 5, 2014, USSS agents seized a Sony Vaio laptop and three other digital devices when they arrested Mr. Seleznev in the Republic of the Maldives. According to Agent LaTulip, at the time of the seizure the Sony Vaio was in a computer bag. (Ex. 1, Affidavit of SA LaTulip). An agent transported the laptop, along with other electronic items seized at the time of arrest, to the USSS Seattle Field Office where the laptop was logged into the evidence vault by Agent Fischlin on July 9, 2014 at 0931. (Ex. 2, Evidence Vault Security Access Log). Although his name does not appear on the evidence vault access log for July 9, 2014, Agent Mills apparently assisted Agent Fischlin in entering the four items into evidence. (Ex. 3, Agent Mills' Notes) (Mills' notes were provided to the defense on January 12, 2016). In his notes – but not in either of his reports regarding the laptop – Agent Mills documents that on July 9, 2014 at approximately 0938 he was looking for the laptop's serial number when "the unit's screen turned on and [he] observed" something unknown. Id. at AGENT_EMAILS_0000830. The sentence cuts off after the word "observed." There is nothing in Mills' notes to indicate whether he turned the computer off at this point or, for some unknown reason, just left it on in the evidence vault. According to the evidence vault access log, Agent Fischlin exited the vault on July 9, 2014 at 1553. See Ex. 2. There is no documentation of when Agent Mills exited the vault because there is no entry in the log documenting that he was in the vault at all on that day.

Over three weeks after the seizure, on July 28, 2014, Agent LaTulip applied for a warrant to search the laptop and other digital devices seized at the time of arrest. (Ex. 1). There is no explanation offered for the delay between the seizure of the laptop and the application for a search warrant. The affidavit in support of the warrant application reviews LaTulip's training and experience and the charges in the Superseding Indictment. As to the condition of the seized items three weeks after they were seized, LaTulip swears that:

> The SUBJECT DEVICES [one of which is the Sony Vaio] are currently in storage at the USSS Seattle Field Office at 2101 4th Avenue, Seattle, Washington 98121. In my training and experience, I know that the SUBJECT DEVICES have been stored in a manner in which their contents are, to the extent material to the investigation, in substantially the same state as they were when the SUBJECT

LAW OFFICES OF JOHN HENRY BROWNE, P.S.
200 DELMAR BUILDING
108 SOUTH WASHINGTON STREET
SEATTLE, WASHINGTON 98104
(206) 388-0777 • FAX: (206) 388-0780

DEVICES first came into the possession of the USSS.
(Ex. 1 at BS SW_0000160).

LaTulip further asserts – again from his training and experience - that internet nicknames (nics) are "jealously guarded," possess status and economic value and thus "may be found on digital devices and electronic storage media used over several years." Id. at 8-9 (164-65). According to the affidavit, the nic "Track2," was suspected of operating carding websites that trafficked in high volumes of stolen access devices. Id. at 4-10 (SW_0000160-66). Agents associated Track2 with Mr. Seleznev, who they alleged hacked over 100 businesses between 2009 and early 2011 and sold hundreds of thousands credit card numbers. Id. at 10-11 (SW_0000166-67). Based on this investigation, a grand jury in the Western District of Washington returned a Superseding Indictment in March 2011, charging Mr. Seleznev with offenses related to harvesting consumer credit card numbers from small business servers and selling them to buyers over the internet. Mr. Seleznev was not arrested until July 5, 2014, a full three years after the Superseding Indictment was filed. Id. 12 (SW_ 0000168).

In attempting to establish a nexus between the electronic devices seized at the time of Mr. Seleznev's arrest and the charges filed in March of 2011, Agent LaTulip asserts that Mr. Seleznev "*may have been* responsible for operating new carding websites that continued to market stolen access devices through the date of his arrest." Id. (emphasis added). LaTulip further alleges that Mr. Seleznev "may have" adopted the new online moniker of "2PAC" – a nic suspected of running a large volume carding forum. In sum, LaTulip asserts that because he knows "that computer hackers often use the same nics and alias names for many years, there is probable cause to believe that Seleznev is still using some or all of those nics and alias names and that evidence of his use of those identities may be located on the … devices." Id.

On January 10, 2012, Mr. Seleznev was indicted in the District of Nevada on allegations of participating in a Racketeer Influenced Corrupt Organization (RICO); conspiracy to engage in a RICO; and two counts of possession of 15 or more unauthorized access devices related to his alleged use of the online nics Track2, Bulba, and nCuX on the forums Carder.su, Carder.info, Crdsu.su; Carder.biz; and Carder.pro—

LAW OFFICES OF JOHN HENRY BROWNE, P.S.
200 DELMAR BUILDING
108 SOUTH WASHINGTON STREET
SEATTLE, WASHINGTON 98104
(206) 388-0777 • FAX: (206) 388-0780

all under the rubric of the Carder.su organization, which sold "dumps" of stolen credit card data. Id. at 27 (183).

The search warrant affidavit La Tulip prepared contains almost no direct information linking Mr. Seleznev and his electronic devices to any alleged criminal activity after January 12, 2012. LaTulip alleges that on February 17, 2013, jchow@bk.ru registered a Liberty Reserve account named "2PAC" and received nearly $10,000.00 from a different Liberty Reserve account agents believed was Mr. Seleznev's. Id. at 33. LaTulip lodges several additional allegations relating to the May 2013 federal and Costa Rican shutdown of Liberty Reserve, an e-currency service, and accounts he suspected were tied to Mr. Seleznev, and then turns his focus to "2pac," who joined the alleged carding forum Omerta.cc on September 25, 2013 and posted an advertisement for 2pac.cc as the "first market of dumps." Id. at 29 (185). Between January 2014 and July 2014, agents purchased several dumps from the website. Id. LaTulip thought that Mr. Seleznev was closely associated with 2PAC and 2pac.cc:

> I believe based on my training and experience that it is *likely* [Seleznev] *or a close associate* created the '2PAC' Liberty Reserve Account and funded it with other accounts controlled by [Seleznev]. I also *believe* that [Seleznev] *or a close associate* created the 2pac.cc domain after bulba.cc was closed to continue carding forum activity. Between the date of [Seleznev's] apprehension on July 5, 2014 and July 21, 2014, the user with the nic "2PAC" did not make any posts on the carding forum 'verified.cm.' Prior to [Seleznev's] arrest, '2PAC' frequently posted comments and/or content on the site. Therefore, I *believe it is likely* that [Seleznev] was the person using the nic '2PAC' and that *someone may have assumed the nic on his behalf* now that he is in custody. I also *believe it is likely* the electronic media obtained from [Seleznev] contains evidence pertaining to carding forums including 2PAC.cc and the nic 2PAC. [Seleznev] would need digital devices to navigate to and manage such domains and to access forums related to carding.

Id. at 33 (189) (emphasis added)

LaTulip explans that there is probable cause to search the subject devices because it is sometimes possible to recover files months or even years after being downloaded, viewed, or deleted, even though it is, by the same token, "technically possible to delete this information." Id. at 36-37 (192-93). LaTulip, finally, claims that because it is, again,

LAW OFFICES OF JOHN HENRY BROWNE, P.S.
200 DELMAR BUILDING
108 SOUTH WASHINGTON STREET
SEATTLE, WASHINGTON 98104
(206) 388-0777 • FAX: (206) 388-0780

possible to recover evidence of a file that had been edited or deleted, there is probable cause to believe that the devices contained timely, relevant evidence. Id. at 37 (193).

B. Forensic Analysis of the Laptop

1. Agent Mills' Interaction with the Laptop

After Agent Mills assisted in the evidence vault on July 9, 2014 and noted that the laptop's screen turned on when he was looking for a serial number, he did not, according to his reports, interact with the laptop again until either July 28, 2014 or July 30, 2014. (Ex. 2, Evidence Vault Security Access Log at USSS_EVID_FORMS_0000094) (Agent Mills entered the evidence vault on July 28, 2014 but did not log what evidence he was reviewing at that time so it is not known whether he handled the laptop at that time). On July 30, 2014, according to his notes, Agent Mills removed the laptop from the evidence vault and observed that the device was powered off. (Ex. 3, Agent Mills' Notes) Then – for unknown reasons – Agent Mills connected the laptop to a Sony AC adapter and began charging the laptop. Id. Charging an electronic device is not a necessary or desired step in imaging the laptop's drive.

Agent Mills reports that when he went to image the computer's solid state drive ("SSD") on August 1, 2014 the "monitor of the laptop turned on and displayed the Windows 8 'splash' screen" when he took the back cover off of the laptop. (Ex. 4, Mills Supplemental Report). Despite indicating in both of his reports that the laptop will not turn off if it has a power supply, Agent Mills claims that he simply "depressed the device's power button and powered the device off" after the splash screen allegedly turned on. (Ex. 3 at AGENT_EMAILS_0000830); see (Ex. 5, Mills Report at 5). He then reports that a later examination of the laptop image revealed Windows registry activity that occurred on August 1, 2014 and was caused by the laptop purportedly waking from a sleep state on that day when the splash screen came on. (Ex. 4 at USSS_0000326).

Once he imaged the SSD Agent Mills noticed that there were "several files in the Windows registry" that had been written after Mr. Seleznev's arrest on July 5, 2014. (Ex. 5, Mills Report at 5). To explain these file changes Agent Mills claims that "Windows remains in a semi-sleep mode in which it is not entirely powered off even if the laptop appears to be powered off or in sleep mode." Id.

LAW OFFICES OF JOHN HENRY BROWNE, P.S.
200 DELMAR BUILDING
108 SOUTH WASHINGTON STREET
SEATTLE, WASHINGTON 98104
(206) 388-0777 • FAX: (206) 388-0780

2. Defense Investigation

Mr. Blank completed his preliminary analysis of the Sony Vaio in late February 2016. In his initial report, Blank explains that it is not simply "several files in the Windows registry," that have last modified dates between July 5, 2014 and August 1, 2014. (Ex. 6, Blank Report). There are 274 files with last modified dates and thousands of files with last access dates that are during the period of time the USSS claims it was storing the Sony Vaio in such a fashion that the data on the laptop would not be altered. (See Ex. 6.1, Graphical Representation of File Activity). This finding calls into question the validity of all of the electronic evidence stored on the laptop. There is no way to definitively determine how the files that were accessed were altered or if alterations were made to other files without changing the last modified or last access dates. Accordingly, "the electronic files now present on the Sony Vaio have been fatally compromised, and cannot now be relied upon in any way." Id.

After Mr. Blank completed his preliminary report the defense experts continued to investigate the July 5, 2014 to July 14, 2014 file activity on the laptop. During that investigation they discovered that the event logs on the SSD do not support Agent Mills' claim that the splash screen came to life on August 1, 2014 when he removed the back off the laptop to reach the SSD. (Ex. 7, Declaration of Eric P. Blank). Why Agent Mills would claim that the splash screen came on to explain file activity on the SSD on August 1, 2014 is unknown.

III. DISCUSSION

A. Information in the Search Warrant Affidavit is Stale

To establish probable cause under the Fourth Amendment, the government must demonstrate that (1) a crime was committed; (2) the defendant committed the crime; and (3) evidence of the crime will be found in the place to be searched. When a search warrant affidavit contains a path of inferences linked one after another it is unlikely that the path will end in probable cause to conduct the desired search. Chism v. Washington State, 661 F.3d 380, 389 (9th Cir. 2011); United States v. Weber, 923 F.2d 1338 (9th Cir. 1991) (while a single inference, standing alone, may be reasonable, "with each succeeding inference, the last reached is less and less likely to be true. Virtual certainty becomes probability, which merges into possibility, which fades into chance"). The facts

LAW OFFICES OF JOHN HENRY BROWNE, P.S.
200 DELMAR BUILDING
108 SOUTH WASHINGTON STREET
SEATTLE, WASHINGTON 98104
(206) 388-0777 • FAX: (206) 388-0780

supporting the affidavit must be "'so closely related to the time of the issue of the warrant as to justify a finding of probable cause at that time.'" United States v. Lacy, 119 F.3d 742, 745-46 (9th Cir.1997) (quoting Durham v. United States, 403 F.2d 190, 193 (9th Cir.1968) (finding that an affidavit based upon facts from four months earlier was stale and thus failed to establish probable cause). The mere lapse of a substantial amount of time, however, is not controlling, and each staleness claim is to be assessed "in light of the particular facts of the case and the nature of the criminal activity and property sought." Id. at 745.

Here, the only somewhat recent information consists of LaTulip's speculation that based upon his training and experience—but not any empirical data—it is "likely" that Mr. Seleznev *or a close associate* created 2pac.cc. Offered to support this conclusion is the fact that for 16 days after Mr. Seleznev's arrest 2PAC did not post any comments on one particular carding forum. From this it seems that after that 16-day period 2PAC started posting again - a direct contradiction of LaTulip's assertion that nics are jealously guarded and not shared. Prior to that, the most recent alleged connection to on-going criminal activity was discovered in May of 2013 when Liberty Reserve records were obtained in an unrelated federal investigation, 14 months prior to the warrant application. (Ex 1, at SW_0000186).

In sum, the affidavit may allege sufficient facts to support a finding of probable cause but all of the critical, non-speculative information was too stale at the time the search warrant issued to justify the search of the electronic devices. See United States v. Greathouse, 297 F.Supp.2d 1264, 1273 (D.Or. 2003) (affiant's statement that child pornography collectors routinely maintain their materials for long periods of time was insufficient to defeat a staleness claim where the statement was not supported by any authority or reference).

B. Delay and Pre-Warrant File Activity

During the 23 days the government maintained custody of the electronic devices prior to seeking a search warrant the evidentiary integrity of the laptop was – either through gross incompetence or intentional actions – compromised to such an extent that suppression is warranted.

LAW OFFICES OF JOHN HENRY BROWNE, P.S.
200 DELMAR BUILDING
108 SOUTH WASHINGTON STREET
SEATTLE, WASHINGTON 98104
(206) 388-0777 • FAX: (206) 388-0780

1. The Delay was Unreasonable under the Fourth Amendment

An unreasonable delay between a warrantless seizure and obtaining a search warrant violates a defendant's rights under the Fourth Amendment. United States v. Sullivan, 797 F.3d 623, 633 (9th Cir. 2015). Courts consider the totality of the circumstances, including whether the individual consented and if the person was under supervision or incarcerated, and must balance the nature and quality of the intrusion against the importance of the governmental interest on a case-by-case basis. Id. (citations omitted). United States v. Dass, 849 F.2d 414 (9th Cir.1988) is illustrative.

In Dass, Hawaiian authorities detained numerous packages for periods ranging from seven to twenty-three days after drug dogs positively alerted to the packages as containing marijuana. Id. at 414. Drawing form Supreme Court and Ninth Circuit precedent that a 29-hour delay between seizure of a mailed package and application for a search warrant was the outer limit of the period of the detention, the Dass Court concluded that the governmental interference was unreasonable. Id. at 415 (citations omitted). The Court admonished that it was reluctant to extend "the outer boundary of 29 hours to a period not measured in hours, but rather in days and weeks." Id. As the Court concluded: "The government's theory would allow an unlimited period of seizure without judicial intervention; to accept its argument would nullify the seizure portion of the search and seizure clause of the fourth amendment." Id. at 635.

Many of the same considerations apply here.

Even more directly on point is United States v. Mitchell, a child pornography case. 565 F.3d 1347 (11th Cir. 2009). The Mitchell Court determined that a 21-day delay between seizing a computer and acquiring a search warrant was unreasonable, and thus suppressed the evidence. The Court first found that because computers are so essential in modern life, detention of a hard drive for three weeks constituted a "significant interference" with the defendant's possessory interest. Id. at 1351. The Court then discounted the defendant's admission that he probably had child pornography on his computers because (1) the computers were likely to contain other, non-contraband evidence and (2) until an agent examines the drive's contents, there is certainty that there is any evidence of illegal activity for the defendant could be lying, factually mistaken, or wrong as a matter of law. Id. at 1351. The Court, lastly, concluded that there was no

LAW OFFICES OF JOHN HENRY BROWNE, P.S.
200 DELMAR BUILDING
108 SOUTH WASHINGTON STREET
SEATTLE, WASHINGTON 98104
(206) 388-0777 • FAX: (206) 388-0780

compelling justification for the delay, the search warrant affidavit was full of boilerplate language, and the government offered no justification for its lack of urgency. Id. at 1352. Given, especially, the nature of a computer hard drive, which is "the digital equivalent of its owner's home, capable of holding a universe of private information," the government must act expediently in acting to protect a defendant's constitutional rights. Id. (citation omitted). Suppression was thus mandated.

In Sullivan, by contrast, because the defendant was a parolee who consented to the search of his laptop—and, in fact, asked police to perform a search to find exculpatory materials—his possessory interest was slight whereas the the government had an overwhelming interest in supervising parolees. Id. at 634. The government, moreover, had a reasonable basis to search insofar as: the laptop likely contained evidence of the defendant's alleged parole violations as well as child pornography; the parole officers who seized the laptop were incapable of performing a forensic computer search; the parole officers transferred the computer to the local police, who then obtained consent to search. Id. None of these factors are present in this case.

In this case, the government offers no explanation for the 23-day delay between the seizure of the electronic devices and the application for a search warrant. Not only does there not appear to be a reason for the delay, during that intervening period of time while the government was responsible for the integrity of the laptop, files were accessed and modified and the computer was handled in ways that are inconsistent with the reports of the investigating agency.

2. Government's Conduct in Handling the Laptop Computer

Where, as here, a defendant seeks a remedy for the government's destruction or loss of evidence, courts balance "'the quality of the Government's conduct' against 'the degree of prejudice to the accused,' where the government bears the burden of justifying its conduct and the accused of demonstrating prejudice." United States v. Sivilla, 714 F.3d 1168, 1173 (9th Cir. 2013) (quoting United States v. Loud Hawk, 628 F.2d 1139, 1152 (9th Cir.1979) (en banc) (Kennedy, J., concurring), overruled on other grounds by United States v. W.R. Grace, 526 F.3d 499, 505-506 (9th Cir. 1998) (en banc)). It is possible, depending upon the situation, that the government's conduct may be so egregious that "only a plausible suggestion of prejudice or none at all would be required

LAW OFFICES OF JOHN HENRY BROWNE, P.S.
200 DELMAR BUILDING
108 SOUTH WASHINGTON STREET
SEATTLE, WASHINGTON 98104
(206) 388-0777 • FAX: (206) 388-0780

for suppression." Loud Hawk, 628 F.2d at 1152. More frequently, however, the government's responsibility for the loss of evidence is caused by negligence, inadvertence, or done intentionally but with an element of good faith so that "a somewhat greater degree of prejudice is tolerated. Id. Where prejudice is severe, "suppression or other sanctions would be appropriate without regard to the good faith or culpability of the government." Id. There is no requirement that a defendant demonstrate bad faith. Sivilla, 714 F.3d at 1173.

United States v. Flyer, 633 F.3d 911 (9th Cir. 2011) is illustrative. In Flyer, the government seized and searched the defendant's Apple laptop and other media, but the forensic examiner erred and allowed his computer's operating system to access the defendant's laptop; he did not report the mistake. Id. at 914-15. The defense forensic analyst found that 6,100 files on the laptop listed last access dates of November 3, 2005—the date of the government's testing—and 63,000 files had last access dates of March 18, 2005, which was after seizure of the laptop. Id. Pursuant to Loud Hawk, the defendant moved to dismiss and suppress based upon the mishandling of the laptop. Id.

Even though the Court cited to Loud Hawk, it nevertheless engaged in a due process analysis, found that the district court did not clearly err in finding no evidence of bad faith, and concluded that the mishandling did not prejudice the defendant. Id. at 916. The Court specifically noted that the government voluntarily dismissed the count based upon evidence the government located on the laptop. Id.

In this case, unlike in Flyer, the damage to the integrity of the SSD is a culmination of repeated acts causing irreconcilable changes to the evidence. On July 9, 2014, while searching for the serial number Mills woke up the computer, observed something which he did not report, and left the system powered. See Exs. 3, 7. On July 30, 2014, he connected the laptop to a power source for unknown reasons having nothing to do with his task of imaging the SSD. See Exs. 3, 7. On August 1, 2014, when Mills went to image the SSD and removed the back cover, he claims to have observed the Windows "splash screen," which the computer logs prove was impossible. Exs. 4, 7. There was, however, file activity on the laptop on August 1, 2014 that is unaccounted for.

In sum, both Mills and Blank agree that the evidence was altered while in the government's custody; Mills' actions, while perhaps merely the result of gross

LAW OFFICES OF JOHN HENRY BROWNE, P.S.
200 DELMAR BUILDING
108 SOUTH WASHINGTON STREET
SEATTLE, WASHINGTON 98104
(206) 388-0777 • FAX: (206) 388-0780

incompetence, nevertheless demonstrates that the government was, at the very least, negligent in "failing to adhere to reasonable standards of care," Sivilla, 714 F.3d at 1173; Exs. 6-7; there is no reasonable justification for Mills' failure to follow proper forensic protocols nor his claims regarding the splash screen coming up on August 1, 2014; and the usefulness of the evidence vault access log in determining the security of the electronic evidence in this case is called into question by Mills entering the vault on July 9, 2014, handling the evidence, and failing to sign in either or out of the vault.

IV. CONCLUSION

For the reasons stated above, the defense respectfully requests that the Court suppress evidence obtained from the Sony Vaio laptop.

DATED this 10th day of May, 2016.

Respectfully submitted,

s/ *John Henry Browne*
JOHN HENRY BROWNE, WSBA #4677

s/ *Emma C. Scanlan*
EMMA C. SCANLAN, WSBA #37835

LAW OFFICES OF JOHN HENRY BROWNE, PS
Attorneys for Roman Seleznev
200 Delmar Building
108 South Washington Street
Seattle, WA 98104
206.388.0777 fax: 206.388.0780
Email: johnhenry@jhblawyer.com
emma@jhblawyer.com

CERTIFICATE OF SERVICE UPON CLIENT

I, LORIE HUTT, hereby certify that on this 10th day of May, 2016, I served this motion and the proposed order on Roman Seleznev by regular U.S. mail addressed to Roman Seleznev, #04385-096, Sea-Tac Federal Detention Center, PO Box 13900, Seattle, WA 98198.

s/ *Lorie J. Hutt*
Lorie J. Hutt, Administrative Assistant

CERTIFICATE OF SERVICE

I hereby certify that on May 10, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of filing to all registered parties.

s/Emma C. Scanlan
Emma C. Scanlan, WSBA #37835

LAW OFFICES OF JOHN HENRY BROWNE, P.S.
200 DELMAR BUILDING
108 SOUTH WASHINGTON STREET
SEATTLE, WASHINGTON 98104
(206) 388-0777 • FAX: (206) 388-0780